

RESEARCH INTEREST

SAST (Static application security testing) on Mobile System/Web Applications; Security and Privacy of Mini-Program Ecosystem; BLE Security.

EDUCATION

- **Shandong University** Qingdao, China
• *Master of Cybersecurity and Information Security; GPA: 86/100* Sept 2021 - June 2024
Advisor: Prof. Wenrui Diao
- **Hebei University** Baoding, China
• *Bachelor of Information Security; GPA: 3.91* Sept 2017 - June 2021
GPA Ranking: 9/110 (Top 8%)
- **Boston University** Boston, MA, USA
• *Visiting Student;* Jan 2020 - Feb 2020

PUBLICATIONS

- **MiniCAT: Understanding and Detecting Cross-Page Request Forgery Vulnerabilities in Mini-Programs**
Zidong Zhang, Qinsheng Hou, Lingyun Ying, Yacong Gu, Rui Li, Wenrui Diao, Shanqing Guo, Haixin Duan
*The ACM Conference on Computer and Communications Security (ACM CCS 2024) *Minor Revision*
- **Living in the Past: Analyzing BLE IoT Devices Based on Mobile Companion Apps in Old Versions**
Jianqi Du, **Zidong Zhang**, Fenghao Xu, Wenrui Diao
The 19th International Conference on Mobility, Sensing and Networking (IEEE MSN 2023)
- **Identifying the BLE Misconfigurations of IoT Devices through Companion Mobile Apps** [Link]
Jianqi Du, Fenghao Xu, Chennan Zhang, **Zidong Zhang**, Xiaoyin Liu, Pengcheng Ren, Wenrui Diao, Shanqing Guo, Kehuan Zhang.
The 19th Annual IEEE International Conference on Sensing, Communication, and Networking (IEEE SECON 2022)

RESEARCH EXPERIENCE

- **QI-ANXIN Research Institute** Beijing, China
• *Security Researcher Intern; Advisor: Dr. Lingyun Ying & Dr. Yacong Gu* Oct 2022 - Now
 - **Mini-Program Analyzing:** Built a mini-programs crawler to crawl 130,000 apps and carried out a large-scale automated measurement for routing security vulnerabilities in mini-programs by using hybrid analysis.
 - **SAST for JavaScript:** Built the static automated vulnerability detection for JavaScript-based applications (e.g., mini-programs) using CodeQL.
 - **Smart IoT Device Security:** Analyzed the protocol and verification process of smart locks and implemented the takeover of any of its devices through its companion mini-programs.

PROJECTS

- **Automated Detection of Mini-Program Vulnerabilities with Hybrid Analysis**
 - Discovered a novel security vulnerability in mini-programs with their routing implementations for the first time.
 - Performed an automated large-scale static analysis of 130,000 mini-programs with CodeQL while using the Xposed Hook for dynamic verification.
 - **Accomplishments:** One paper in submission(ACM CCS '24); 3 vulnerabilities confirmed by CNVD.
- **Analyzing BLE Devices with Older Versions of Companion Apps**
 - Analyzed BLE devices that could not be OTA upgraded via old version of their companion apps.
 - Designed an automated tool to perform large-scale automatic measurements in IoT App datasets to measure the security risks from older versions of apps for devices that do not support OTA upgrades.
 - **Accomplishments:** One paper accepted (IEEE MSN '23); 3 vulnerabilities under CVE review.
- **Identifying the BLE Misconfigurations of IoT Devices through Companion Apps**
 - Based on the static analysis, defined a set of strategies for detecting misconfiguration in the companion app of BLE devices.
 - Designed an automatic analysis tool to detect the BLE misconfigurations based on pre-defined checking strategies from 4,589 companion apps.
 - **Accomplishments:** One paper published. (IEEE SECON '22)

TEACHING

- **Teaching Assistant** Qingdao, China
 - **Software Security:** Instructor: Prof. Wenrui Diao (2021 Fall)
 - **Reverse Engineering:** Instructor: Prof. Wenrui Diao (2023 Spring)

HONORS AND AWARDS

- DataCon Security Analysis Competition, Vulnerability Analysis Track, Third Place (3/689 teams) - Nov. 2023
- The Mathematical Contest in Modeling (MCM), Meritorious Winner - April 2020
- National College Student Information Security Contest (CISCN), First Prize of North China Region - Sept. 2020
- National College Student Information Security Contest (CISCN), Second Prize of North China Region - June 2019
- College Student Information Security Contest in Hebei Province, First Prize - October 2019

VULNERABILITIES DISCLOSURES

- WeChat Mini Program Privilege Escalation Vulnerability. (CNVD-2023-75836, CNVD-2023-75837)
- Nankai University Original Vulnerability Reporting Certificate. (EDUSRC-NKU-2019-0074)
- Shanghai Jiaotong University Original Vulnerability Reporting Certificate. (EDUSRC-2019-0217)
- Shanghai International Studies University Original Vulnerability Reporting Certificate. (SISUVD-2019074)
- Alibaba SRC Submission (1 High Severity), Butian SRC Submission (2 High Severity, 3 Medium Severity).

TECHNICAL SKILLS

- **Development:** Python, PHP, JavaScript, Lua, C++, BLE Development (for Android).
- **Security tools:** CodeQL, Xposed, Frida, Android Reverse(Jadx), IDA Pro, Burpsuite, Nmap, Metasploit.